UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

LINDEN BUZZELL, individually and on behalf of all others similarly situated,

Plaintiff,

v.

MAXIMUS, INC. and MAXIMUS FEDERAL SERVICES, INC.,

Defendants.

Civil Action No.: 1:23-cv-1028

CLASS ACTION COMPLAINT

Plaintiff Linden Buzzell ("Plaintiff"), individually and on behalf of a class of similarly situated persons, brings this Class Action Complaint and alleges the following against defendants Maximus, Inc. and Maximus Federal Services, Inc. (collectively "Maximus" or "Defendants"), based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Maximus for its failure to properly secure Plaintiff's and Class Members' personally identifiable information ("PII") and personal health information ("PHI"). The PII and PHI may have included victims' names, Social Security numbers, dates of birth, contact information, driver's license numbers, health insurance information, medical histories, and healthcare provider and prescription information.

2. Maximus failed to comply with industry standards to protect information systems that contain PII and PHI. Plaintiff seeks, among other things, orders requiring Maximus to fully

and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the disclosure (the "Data Breach") in the future.

3. Maximus uses MOVEit Transfer ("MOVEit") to exchange files and data between servers, systems and applications. Maximus claims that, on May 30, 2023, it "detected unusual activity in [its] MOVEit environment," and that MOVEit's developer disclosed the following day that unauthorized parties had exploited a vulnerability in the software to gain access to the files of multiple MOVEit users.

4. On June 7, 2023, government officials confirmed that the "CL0P Ransomware Gang" ("CL0P") was the unauthorized parties.

5. But Maximus did not disclose that its data was affected until July 26, 2023, when it filed a report with the Securities and Exchange Commission ("SEC") reflecting that the PII and PHI "of at least 8 to 11 million individuals" in its files were exposed to CL0P (the "Data Breach").

6. Maximus could have prevented the recent Data Breach had it implemented adequate vendor screening, and maintained adequate data security measures and protocols in order to secure and protect Plaintiff's and Class Members' data.

7. As a vendor providing electronic health record and cloud-based storage services to customers that collect and store PHI, Maximus knowingly obtains sensitive PII and PHI and has a resulting duty to securely maintain that information in confidence. Plaintiff and Class Members would not have provided their PII and PHI to Maximus customers if they had known that Maximus would not ensure that it used adequate security measures.

8. Plaintiff seeks to remedy these harms individually and on behalf of all other similarly situated individuals whose PII and/or PHI were stolen in the Data Breach. Plaintiff seeks remedies including compensation for time spent responding to the Data Breach and other types of harm, free credit monitoring and identity theft insurance, and injunctive relief including substantial improvements to Maximus's data security policies and practices.

PARTIES

9. Plaintiff Linden Buzzell is a Maine resident who is insured by Medicare. Plaintiff received a letter from defendant Maximus Federal Services, Inc. and the Centers for Medicare and Medicaid Services dated July 28, 2022. That letter reflects that Mr. Buzzell's "personal and Medicare information was involved" in the Data Breach, and the "information may have included the following:

- Name
- Social Security Number or Individual Taxpayer Identification Number
- Date of Birth
- Mailing Address
- Telephone Number, Fax Number, & Email Address
- Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
- Driver's License Number and State Identification Number
- Medical History/Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.)
- Healthcare Provider and Prescription Information
- Health Insurance Claims and Policy/Subscriber Information

- Health Benefits & Enrollment Information."[1]

10. Defendant Maximus, Inc. is a Virginia corporation, with its principal place of business in McLean, Virginia.

11. Defendant Maximus Federal Services, Inc. is a Virginia corporation, with its principal place of business in McLean, Virginia. Maximus Federal Services, Inc. is a subsidiary of defendant Maximus, Inc.

JURISDICTION AND VENUE

12. This Court subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Maximus, there are more than 100 class members, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

13. This Court has personal jurisdiction over Maximus because Maximus maintains its principal place of business in Virginia and conducts substantial business in this District through its principal place of business; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District.

14. Venue is proper in this Court and Division pursuant to 28 U.S.C. § 1391(b)(1) and (2) because Maximus resides in this District, and this District is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred.

[1] Ex. 1, Notice Letter, at 1-2.

FACTUAL ALLEGATIONS

The Data Breach

15. Maximus maintains offices in ten countries, and describes its business as "partner[ing] with state, federal and local governments to provide communities with critical health and human service programs."[2] Due to the nature of the services it provides, Maximus acquires and electronically stores PII and PHI. Maximus was therefore required to ensure that PII and PHI were not disclosed or disseminated to unauthorized third parties without Plaintiff's and Class Members' express written consent.

16. Maximus claims that, on May 30, 2023, it "detected unusual activity in [its] MOVEit environment."[3] Maximus further claims that the following day "the developer of MOVEit … announced a … vulnerability in the application that allowed unauthorized third parties to access its customers' MOVEit environments."[4]

17. July 26, 2023, Maximus filed a report with the Securities and Exchange Commission ("SEC") reflecting that the PII and PHI "of at least 8 to 11 million individuals" in its files were exposed to CL0P (the "Data Breach").[5] But Maximus has not apparently posted a notice of the Data Breach on its website. Nor has it reported the incident to the U.S. Department of Health and Human Services Office for Civil Rights, as is required by law, or made any

[2] "Better solutions for better lives," available at https://maximus.com/our-company (last visited August 2, 2023).

[3] Maximus form notification letter, July 28, 2023, available at https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-488.pdf (last visited August 2, 2023).

[4] Maximus, Inc. Form 8-K, July 26, 2023, available at https://www.sec.gov/ix?doc=/Archives/edgar/data/1032220/000103222023000061/mms-20230726.htm (last visited August 2, 2023).

[5] *Id.*

disclosure to the governments of any of several states in which affected individuals may be located.

18. Maximus's disclosures are otherwise deficient. They do not include basic details concerning the Data Breach, including, but not limited to, why PII and PHI were stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the data was encrypted or otherwise protected, and what Maximus knows about the degree to which the data has been disseminated.

19. Maximus has not nearly disclosed all the details of the Data Breach and its investigation. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, Maximus has taken to secure the PII and PHI still in its possession. Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses the harm to Plaintiff's and Class Members' interests, and ensure that Maximus has proper measures in place to prevent similar incidents from occurring in the future.

Maximus's Privacy Policies

20. The Health Insurance Portability and Accountability Act ('HIPAA') requires that Maximus maintain strict privacy practices. Maximus provides services to Plaintiff and other Maine Medicare recipients. A Maine Department of Health and Human Services document on Maximus's website reflects that "INFORMATION GATHERED FROM ANY SOURCE DURING THE ASSESSMENT PROCESS MUST BE TREATED AS CONFIDENTIAL

HIPAA AND OTHER FEDERAL AND STATE LAWS AND REGULATIONS GOVERN DISCLOSURE OF CONFIDENTIAL INFORAMTION [sic]." [6]

21. A Maximus Privacy Statement directed to Maine residents claims that "Maximus maintains policies that protect the confidentiality of personal information obtained in the course of its regular business functions. Maximus privacy policies impose a number of standards to guard the confidentiality, prohibit the unlawful disclosure, and limit access to personal information (such as Social Security Numbers and Medicaid ID numbers). Maximus safeguards personal information by having physical, technical, and administrative safeguards in place."[7]

The Healthcare Sector is a Primary Target for Data Breaches

22. Maximus was on notice that companies in the healthcare industry are susceptible targets for data breaches.

23. Maximus was also on notice that the Federal Bureau of Investigation has been concerned about data security in the healthcare industry. On April 8, 2014, the FBI's Cyber Division issued a Private Industry Notification to companies within the healthcare sector, stating that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and pointed out that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise." The same warning specifically

[6] MED Referral Instructions, at 2 (capitals in original) available at https://maximus.com/sites/default/files/svcs/documents/ME-ASA-Med-Referral-Instructions-Update%2009.26.18.pdf (last visited August 2, 2023).

[7] Maximus Federal Portal for Maine Surprise Bill Independent Dispute Resolution Privacy Statement, at 2, available at https://dispute.maximus.com/me/resource/1614634710000/PrivacyPolicy (last visited August 2, 2023).

noted that "[t]he FBI has observed malicious actors targeting healthcare-related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or PII."[8]

24. The number of reported North American data breaches increased by over 50 percent in 2021, from 1,080 in 2020[9], to 1,638 in 2021.[10] As a recent report reflects, "[h]ealthcare has increasingly become a target of run-of-the-mill hacking attacks and the more impactful ransomware campaigns."[11]

25. At the end of 2018, the healthcare sector ranked second in the number of data breaches among measured sectors, and had the highest rate of exposure for each breach.[12] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[13] Almost 50 percent of the victims lost their healthcare coverage as a result of the

---

[8] Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain (Apr. 8, 2014), FBI Cyber Division Private Industry Notification (available at https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf) (last accessed Mar. 14, 2023).

[9] *See* Verizon 2021 Data Breach Investigations Report, at 97, https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf (last accessed Mar. 14, 2023).

[10] *See* Verizon 2022 Data Breach Investigations Report, at 83 (available at https://www.verizon.com/ business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf) (last accessed Mar. 14, 2023).

[11] *Id.* at 62.

[12] *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center (available at https://www.idtheftcenter.org/2018-data-breaches) (last accessed Mar. 14, 2023).

[13] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) (available at https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/) (last accessed Mar. 14, 2023).

incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy.[14]

26. Healthcare-related breaches have persisted because criminals see electronic patient data as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the previous 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[15] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[16]

27. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[17]

---

[14] *Id.*

[15] *2019 HIMSS Cybersecurity Survey* (available at https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf) (last accessed Mar. 14, 2023).

[16] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Apr. 4, 2019 (available at https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks) (last accessed Mar. 14, 2023).

[17] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019) (available at https://www.ama-assn.org/practice-

28. As a major healthcare services provider, Maximus knew, or should have known, the importance of safeguarding Plaintiff's and Class Members' PII and PHI entrusted to it and of the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on Plaintiff and Class Members by virtue of a breach. Maximus failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Maximus Stores Plaintiff's and Class Members' PII and PHI

29. Maximus obtains and stores a massive amount of PII and PHI. As a condition of engaging in health care services, Maximus customers require that patients entrust them with highly confidential PII and PHI.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Maximus assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from disclosure.

31. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and rely on Maximus to keep this information confidential and securely maintained, and to make only authorized disclosures of this information.

PII and PHI are Valuable and Subject to Unauthorized Disclosure

32. Maximus was aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

33. PII and PHI are valuable commodities to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft,

---

management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals) (last visited Mar. 14, 2023).

and medical and financial fraud.[18] Indeed, a robust illegal market exists in which criminals openly post stolen PII and PHI on multiple underground websites, commonly referred to as the "dark web." PHI can sell for as much as $363 on the dark web, according to the Infosec Institute.[19]

34. PHI is particularly valuable because criminals can use it to target victims with frauds and swindles that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

35. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's PHI is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[20]

36. The ramifications of Maximus's failure to keep Plaintiff's and Class Members' PII and PHI secure are long-lasting and severe. Once PII and PHI are stolen, fraudulent use of

[18] Federal Trade Commission, What To Know About Identity Theft (available at https://consumer.ftc.gov/articles/what-know-about-identity-theft) (last accessed Mar. 14, 2023).

[19] Center for Internet Security, *Data Breaches: In the Healthcare Sector* (available at https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/) (last accessed Mar. 14, 2023).

[20] Michael Ollove, The Rise of Medical Identity Theft in Healthcare, Kaiser Health News (Feb. 7, 2014) (available at https://khn.org/news/rise-of-indentity-theft/) (last accessed Mar. 14, 2023).

that information and damage to victims may continue for years. Fraudulent activity might not show up for months or even years thereafter.

37. Further, criminals often trade stolen PII and PHI for years following a breach. Cybercriminals can post stolen PII and PHI on the internet, thereby making such information publicly available.

38. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [21] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[22]

39. Maximus knew, or should have known, the importance of safeguarding PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Plaintiff and Class Members because of a breach. Maximus failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

The Data Breach Exposed Plaintiff and Class Members to Identity Theft and Out-of-Pocket Losses

40. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of their rights. They are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

---

[21] *See* Medical ID Theft Checklist (available at https://www.identityforce.com/blog/medical-id-theft-checklist-2) (last accessed Mar. 14, 2023).

[22] Experian, The Potential Damages and Consequences of Medical Identityy Theft and Healthcare Data Breaches (available at https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf) (last accessed Mar. 14, 2023).

41. Despite all the publicly available knowledge of known and foreseeable consequences of the disclosure of PII and PHI, Maximus's policies and practices with respect to maintaining the security of Plaintiff's and Class Members' PII and PHI were reckless, or at the very least, negligent.

42. In virtually all contexts, the expenditure of time has consistently been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be compensated for the time they have expended because of Maximus's misfeasance.

43. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[23]

44. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer financial loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their PII and PHI;

b. identity theft and fraud resulting from the theft of their PII and PHI;

c. costs associated with the detection and prevention of identity theft;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

[23] 2014 LexisNexis True Cost of Fraud Study (available at https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf) (last accessed Mar. 14, 2023).

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

g. the continued imminent injury flowing from potential fraud and identify theft posed by their PII and PHI being in the possession of one or more unauthorized third parties.

Maximus's Lax Security Violates HIPAA

45. Maximus had a non-delegable duty to ensure that all PHI it collected and stored was secure.

46. Maximus is bound by HIPAA (*see* 45 C.F.R. § 160.102) and, as a result, is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

47. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. See 45 C.F.R. § 160.103.

48. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

49. HIPAA requires that Maximus implement appropriate safeguards for this information.

50. Despite these requirements, Maximus failed to comply with its duties under HIPAA and its own Privacy Practices. In particular, Maximus failed to:

a. maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. adequately protect Plaintiff's and Class Members' PHI;

c. ensure the confidentiality and integrity of electronic PHI created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. ensure compliance with the electronic PHI security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. train all members of its workforce effectively on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their responsibilities and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b)

51. Maximus failed to comply with its duties under HIPAA despite being aware of the risks associated with unauthorized access to Plaintiff's and Class Members' PHI.

Maximus Violated FTC Guidelines

52. The Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, prohibited Maximus from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' PII is an "unfair practice" in violation of the FTC Act. *See, e.g., Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

53. The FTC has promulgated several guides for businesses that reflect the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[24]

[24] Federal Trade Commission, Start With Security: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last accessed Mar. 14, 2023).

54. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established data security guidelines for businesses.[25] The guidelines reflect that businesses should protect the PII that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to confidential data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[26]

56. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. Maximus failed to properly implement basic data security practices. Maximus's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

[25] Federal Trade Commission, Protecting Personal Information: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last accessed Mar. 14, 2023).

[26] FTC, *Start With Security*, *supra*.

58. Maximus was at all times fully aware of its obligation to protect Plaintiff's and Class Members' PII and PHI because of its position as a healthcare provider. Maximus was also aware of the significant repercussions that would result from its failure to do so.

CLASS ACTION ALLEGATIONS

59. Pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, Plaintiff seeks certification of a Class as defined below:

> All persons in the United States and its territories whose PII and/or PHI was compromised in the Data Breach.

60. Excluded from the Class are Maximus, any entity in which Maximus has a controlling interest, and Maximus's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

61. Plaintiff reserves the right to modify or amend the definition of the proposed Class as additional information becomes available to Plaintiff.

62. **Numerosity:** The Class Members are so numerous that individual joinder of all Class Members is impracticable. Maximus has disclosed that the Data Breach affected 8 to 11 million individuals. All Class Members' names and addresses are available from Maximus's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

63. **Commonality:** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Maximus had a duty to protect the PII and PHI of Class Members;

b. Whether Maximus was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI;

c. Whether Maximus had duties not to disclose the PII and PHI of Class Members to unauthorized third parties;

d. Whether Maximus took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII and PHI;

e. Whether Maximus failed to adequately safeguard the PII and PHI of Class Members;

f. Whether Maximus failed to implement and maintain reasonable security policies and practices appropriate to the nature and scope of the PII and PHI compromised in the Data Breach;

g. Whether Maximus adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

h. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or punitive damages because of Maximus's wrongful conduct;

i. Whether Plaintiff and Class Members are entitled to restitution because of Maximus's wrongful conduct;

j. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm they face because of the Data Breach; and

k. Whether Plaintiff and Class Members are entitled to identity theft protection for their respective lifetimes.

64. **Typicality:** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII and PHI, like that of every other Class Member, was disclosed by Maximus.

Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through Maximus's common misconduct. Plaintiff is advancing the same claims and legal theories individually and on behalf of all other Class Members, and there are no defenses that are unique to Plaintiff. Plaintiff's claims and Class Members' claims arise from the same operative facts and are based on the same legal theories.

65. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Maximus to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's counsel are competent and experienced in litigating class actions, including extensive experience in data breach litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

66. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Maximus has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Maximus's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Maximus's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

67. **Superiority:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and

expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Maximus. Even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

68. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Maximus would necessarily gain an unconscionable advantage in non-class litigation, since Maximus would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by Class Members and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

69. The litigation of Plaintiff's claims is manageable. Maximus's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with maintenance of this lawsuit as a class action.

70. Adequate notice can be given to Class Members directly using information maintained in Maximus's records.

71. Unless a class-wide injunction is issued, Maximus may continue to maintain inadequate security with respect to the PII and PHI of Class Members, Maximus may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Maximus may continue to act unlawfully as set forth in this Complaint.

72. Maximus has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

COUNT I
NEGLIGENCE
(on behalf of Plaintiff and the Class)

73. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

74. Maximus knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII and PHI, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. That duty included, among other things, designing, maintaining, and testing Maximus's security protocols to ensure that Plaintiff's and Class Members' PII and PHI in Maximus's possession was adequately secured and protected, that Plaintiff's and Class Members' PII and PHI on Maximus's networks were not accessible to criminals without authorization, and that Maximus employees tasked with maintaining such information were adequately trained on security measures regarding the security of Plaintiff's and Class Members' PII and PHI.

75. Plaintiff and Class Members entrusted their PII and PHI to Maximus with the understanding that Maximus would safeguard their information, use their PII and PHI for business purposes only, and not disclose their PII and PHI to unauthorized third parties.

76. Maximus knew or reasonably should have known that a failure to exercise due care in the collecting, storing, and using Plaintiff's and Class Members' PII and PHI involved an unreasonable risk of harm to Plaintiff and Class Members.

77. Maximus also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII and PHI.

78. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of prior data breaches and disclosures prevalent in today's digital landscape, including the explosion of data breaches involving similarly situated healthcare providers.

79. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Maximus knew or should have known of the inherent risks in collecting and storing Plaintiff's and Class Members' PII and PHI, the critical importance of providing adequate security of that information, the necessity for encrypting PHI stored on Maximus's systems, and that it had inadequate IT security protocols in place to secure Plaintiff's and Class Members' PII and PHI.

80. Maximus's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Maximus's misconduct included, but was not limited to, failure to take the steps and opportunities to prevent the Data Breach as set forth herein.

81. Plaintiff and Class Members had no ability to protect their PII and PHI that was in Maximus's possession.

82. Maximus was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

83. Maximus had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' PII and PHI within its possession was compromised and precisely the type(s) of information that were compromised.

84. Maximus had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII and PHI.

85. Maximus systematically failed to provide adequate security for data in its possession.

86. Maximus, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII and PHI within its possession.

87. Maximus, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII and PHI.

88. Maximus, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII and PHI within Maximus's possession might have been compromised and precisely the type of information compromised.

89. Maximus's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII and PHI to be compromised.

90. But for all of Maximus's acts of negligence detailed above, including allowing cyber criminals to access its systems containing Plaintiff's and Class Members' PII and PHI would not have been compromised.

91. Plaintiff never transmitted his own unencrypted PHI over the internet or any other unsecured source.

92. Following the Data Breach, Plaintiff's PHI has been seized by unauthorized third parties who are now free to exploit and misuse that PHI without any ability for Plaintiff to recapture and erase that PHI from further dissemination—Plaintiff's PHI is forever compromised.

93. But for the Data Breach, Plaintiff would not have incurred the loss and publication of his PHI and other injuries.

94. There is a close causal connection between Maximus's failure to implement security measures to protect Plaintiff's and Class Members' PII and PHI and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members. Plaintiff's and Class Members' PHI was accessed and compromised as the proximate result of Maximus's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures and encryption.

95. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, loss of privacy, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

96. As a result of Maximus's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII and PHI, which is still in the possession of third parties, will be used for fraudulent purposes.

97. Plaintiff seeks the award of actual damages on behalf of themselves and the Class.

98. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling Maximus to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Maximus to provide detailed and

specific disclosure of what types of PII and PHI have been compromised as a result of the data breach.

COUNT II
NEGLIGENCE PER SE
(on behalf of Plaintiff and the Class)

99. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

100. Pursuant to HIPAA (42 U.S.C. § 1302d et seq.) and the FTC Act, Maximus was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' PHI and PII.

101. Maximus breached its duties by failing to employ industry standard data and cybersecurity measures to ensure its compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

102. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiff's and Class Members' PII and PHI in compliance with applicable laws would result in an unauthorized third-party gaining access to Maximus's networks, databases, and computers that stored or contained Plaintiff's and Class Members' PII and PHI.

103. Plaintiff's and Class Members' PII and PHI constitute personal property that was stolen due to Maximus's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

104. Maximus's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted PII and PHI, and Plaintiff and Class Members have suffered and will continue to suffer damages as a

result of Maximus's conduct. Plaintiff and Class Members seek damages and other relief as a result of Maximus's negligence.

COUNT III
BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiff and the Class)

105. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

106. When Plaintiff and Class Members provided their PII and PHI to Maximus, they entered into implied contracts with Maximus, under which Maximus agreed to take reasonable steps to protect Plaintiff's and Class Members' PII and PHI, comply with it statutory and common law duties to protect Plaintiff's and Class Members' PII and PHI, and to timely notify them in the event of a data breach.

107. Maximus solicited and invited Plaintiff and Class Members to provide their PII and PHI as part of Maximus's provision of healthcare support services. Plaintiff and Class Members accepted Maximus's offers and provided their PII and PHI to Maximus.

108. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that Maximus's data security practices complied with its statutory and common law duties to adequately protect Plaintiff's and Class Members' PII and PHI and to timely notify them in the event of a data breach.

109. Maximus's implied promise to safeguard PII and PHI is evidenced by, *e.g.*, the representations in Maximus's privacy policies set forth above.

110. Plaintiff and Class Members would not have provided their PII and PHI to Maximus had they known that Maximus would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

111. Plaintiff and Class Members fully performed their obligations under their implied contracts with Maximus.

112. Maximus breached its implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' PII and PHI and by failing to provide them with timely and accurate notice of the Data Breach.

113. The losses and damages Plaintiff sustained, include, but are not limited to:

a. Theft of their PII and PHI;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling, and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Maximus with the mutual understanding that Maximus would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and PHI, which remains in Maximus's possession and is subject to further breaches so long as Maximus fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

114. As a direct and proximate result of Maximus's breach of contract, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT IV
BREACH OF CONFIDENCE
(on behalf of Plaintiff and the Class)

115. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

116. Plaintiff and Class Members have an interest, both equitable and legal, in their PII and PHI that was conveyed to, collected by, and maintained by Maximus and that was accessed or compromised in the Data Breach.

117. Maximus was provided with and stored private and valuable PHI related to Plaintiff and the Class, which it was required to maintain in confidence.

118. Plaintiff and the Class provided Maximus with their personal and confidential PHI under both the express and/or implied agreement of Maximus to limit the use and disclosure of such PHI.

119. Maximus owed a duty to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PHI in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

120. Maximus had an obligation to maintain the confidentiality of Plaintiff's and Class Members' PHI.

121. Plaintiff and Class Members have a privacy interest in their personal medical matters, and Maximus had a duty not to disclose their confidential medical information.

122. As a result of the parties' relationship, Maximus had possession and knowledge of confidential PHI and confidential medical records of Plaintiff and Class Members.

123. Plaintiff's and Class Members' PHI is not generally known to the public and is confidential by nature.

124. Plaintiff and Class Members did not consent to nor authorize Maximus to release or disclose their PHI to unknown criminal actors.

125. Maximus breached the duties of confidence it owed to Plaintiff and Class Members when Plaintiff's and Class Members' PHI was disclosed to unknown criminal hackers.

126. Maximus breached its duties of confidence by failing to safeguard Plaintiff's and Class Members' PHI, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII

and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to Plaintiff and Class Members; (h) storing PHI and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class Members' PHI and medical records/information to a criminal third party.

127. But for Maximus's wrongful breach of its duty of confidences owed to Plaintiff and Class Members, their privacy, confidences, and PHI would not have been compromised.

128. As a direct and proximate result of Maximus's breach of Plaintiff's and Class Members' confidences, Plaintiff and Class Members have suffered injuries, including:

a. Loss of their privacy and confidentiality in their PHI;

b. Theft of their PII and PHI;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

h. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Maximus with the mutual understanding that Maximus would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

i. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Maximus's possession and is subject to further breaches so long as Maximus fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

j. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Maximus; and

j. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PHI.

129. Additionally, Maximus received payments from Plaintiff and Class Members for services with the understanding that Maximus would uphold its responsibilities to maintain the confidences of Plaintiff's and Class Members' private medical information.

130. Maximus breached the confidence of Plaintiff and Class Members when it made an unauthorized release and disclosure of their confidential medical information and/or PHI and, accordingly, it would be inequitable for Maximus to retain the benefit at Plaintiff's and Class Members' expense.

131. As a direct and proximate result of Maximus's breach of its duty of confidences, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT V
UNJUST ENRICHMENT
(on behalf of Plaintiff and the Class)

132. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

133. Plaintiff and Class Members have an interest, both equitable and legal, in their PHI and PII that was conferred upon, collected by, and maintained by Maximus and that was stolen in the Data Breach.

134. Maximus benefitted from the conferral upon it of Plaintiff's and Class Members' PII and PHI, and by its ability to retain and use that information. Maximus understood that it so benefitted.

135. Maximus also understood and appreciated that Plaintiff's and Class Members' PHI and PII was private and confidential and that its value depended upon Maximus maintaining its privacy and confidentiality.

136. But for Maximus's willingness and commitment to maintain its privacy and confidentiality, that PHI and PII would not have been transferred to and entrusted with Maximus. Further, if Maximus had disclosed that its data security measures were inadequate, Maximus would not have been permitted to continue in operation by regulators and the healthcare marketplace.

137. As a result of Maximus's wrongful conduct as alleged in this Complaint (including, among other things, its failure to employ adequate data security measures, its continued maintenance and use of Plaintiff's and Class Members' PHI without having adequate data security measures, and its other conduct facilitating the theft of that PHI and PII), Maximus has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

138. Maximus's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compilation and use of Plaintiff's and Class Members' sensitive PHI and PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers.

139. Under the common law doctrine of unjust enrichment, it is inequitable for Maximus to be permitted to retain the benefits it received, and is still receiving, without justification, from the use of Plaintiff's and Class Members' PHI and PII in an unfair and unconscionable manner. Maximus's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

140. The benefit conferred upon, received, and enjoyed by Maximus was not conferred officiously or gratuitously, and it would be inequitable and unjust for Maximus to retain the benefit.

COUNT VI
INJUNCTIVE/DECLARATORY RELIEF
(on behalf of Plaintiff and the Class)

141. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

142. Maximus owes a duty of care to Plaintiff and Class Members requiring it to adequately secure PII and PHI.

143. Maximus still stores Plaintiff's and Class Members' PII and PHI.

144. Since the Data Breach, Maximus has announced no specific changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent similar incidents from occurring in the future.

145. Maximus has not satisfied its legal duties to Plaintiff and Class Members.

146. Actual harm has arisen in the wake of the Data Breach regarding Maximus's duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and PHI, and Maximus's failure to address the security failings that led to that exposure.

147. Plaintiff, therefore, seeks a declaration: (a) that Maximus's existing security measures do not comply with its duties of care to provide adequate security; and (b) that to comply with its duties of care, Maximus must implement and maintain reasonable security measures, including, but not limited to, the following:

a. ordering that Maximus engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Maximus's systems on a periodic basis, and ordering

Maximus to promptly correct any problems or issues detected by such third-party security auditors;

b. ordering that Maximus engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Maximus audit, test, and train its security personnel regarding any new or modified procedures;

d. ordering that Maximus segment PHI by, among other things, creating firewalls and access controls so that if one area of Maximus's system is compromised, hackers cannot gain access to other portions of Maximus's systems;

e. ordering that Maximus purge, delete, and destroy in a reasonably secure manner PII and PHI not necessary for its provision of services;

f. ordering that Maximus conduct regular computer system scanning and security checks; and

g. ordering that Maximus routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, prays for relief as follows:

a. for an Order certifying the Class as defined herein, and appointing Plaintiff and his counsel to represent the Class;

b. for equitable relief enjoining Maximus from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and

Class Members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

c. for equitable relief compelling Maximus to use appropriate cyber security methods and policies with respect to PII and PHI collection, storage, and protection, and to disclose with specificity to Class Members the types of PII and PHI compromised;

d. for an award of damages, including actual, nominal, consequential, enhanced compensatory, and punitive damages, as allowed by law in an amount to be determined;

e. for an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. for prejudgment interest on all amounts awarded; and

g. such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: August 2, 2023

Respectfully submitted,

KELLY GUZZO PLC

/s/ Kristi C. Kelly

Kristi C. Kelly, VSB #72791
Andrew J. Guzzo, VSB #82170
Casey S. Nash, VSB #84261
J. Patrick McNichol, VSB #92699
KELLY GUZZO, PLC
3925 Chain Bridge Road, Suite 202
Fairfax, VA 22030
Telephone: (703) 424-7572
Facsimile: (703) 591-0167
Email: kkelly@kellyguzzo.com
Email: aguzzo@kellyguzzo.com
Email: casey@kellyguzzo.com
Email: pat@kellyguzzo.com

BAILEY GLASSER LLP
John W. Barrett
209 Capitol Street
Charleston, WV 25301
(304) 345-6555
jbarrett@baileyglasser.com

BAILEY GLASSER LLP
Bart D. Cohen
Lawrence J. Lederer
1622 Locust Street
Philadelphia, PA 19103
(215) 274-9420
bcohen@baileyglasser.com
llederer@baileyglasser.com

THE CONSUMER PROTECTION FIRM, PLLC
William "Billy" Peerce Howard
401 East Jackson Street, Suite 2340
Truist Place
Tampa, FL 33602
(813) 500-1500
Billy@TheConsumerProtectionFirm.com

Attorneys for Plaintiff and the Proposed Class